

provide adequate protection and prevent access by unauthorized persons;

(c) Act on all suggestions and complaints concerning the Commission's information security program;

(d) Recommend appropriate administrative action to correct abuse or violations of any provision of Executive Order 12356; and

(e) Consider and decide other questions concerning classification and declassification that may be brought before it.

§ 503.54 Original classification.

(a) No Commission Member or employee has the authority to classify any Commission originated information.

(b) If a Commission Member or employee develops information that appears to require classification, or receives any foreign government information as defined in § 503.51(f), the Member or employee shall immediately notify the Security Officer and appropriately protect the information.

(c) If the Security Officer believes the information warrants classification, it shall be sent to the appropriate agency with original classification authority over the subject matter, or to the Information Security Oversight Office, for review and a classification determination.

(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority.

§ 503.55 Derivative classification.

(a) Any document that includes paraphrases, restatements, or summaries of, or incorporates in new form, information that is already classified, shall be assigned the same level of classification as the sources, unless consultation with originators or instructions contained in authorized classification guides indicate that no classification, or a lower classification than originally assigned, should be used.

(b) Persons who apply derivative classification markings shall:

(1) Observe and respect original classification decisions, and

(2) Carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

(c) A derivative document that derives its classification from the approved use of the classification guide of another agency shall bear the declassification date required by the provisions of that classification guide.

(d) Documents classified derivatively on the basis of source documents or classification guides shall bear all applicable marking prescribed in sections 2001.5(a) through 2001.5(e), Information Security Oversight Office Directive No. 1.

(1) *Classification authority.* The authority for classification shall be shown as follows:

(i) *Classified by (description of source documents or classification guide), or*

(ii) *Classified by multiple sources*, if a document is classified on the basis of more than one source document or classification guide.

(iii) In these cases, the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis of a source document that is marked "Classified by Multiple Sources" shall cite the source document in its "Classified by" line rather than the term "Multiple sources."

(2) *Declassification and downgrading instructions.* Date or events for automatic declassification or downgrading, or the notation "Originating Agency's Determination Required" to indicate that the document is not to be declassified automatically, shall be carried forward from the source document, or as directed by a classification guide, and shown on "declassify on" line as follows:

"Declassify on: (date, description of event);
or
"Originating Agency's Determination Required (OADR)."